The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/11/2010

SUBJECT:
Multiple Vulnerabilities Discovered in Adobe Products

OVERVIEW:
Six vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR. Adobe Flash Player is a widely distributed multimedia and application player for Microsoft Windows, Mozilla, and Apple systems. Adobe AIR is a cross-platform runtime for developing Internet applications on the desktop. These vulnerabilities can be exploited if a user visits a website hosting malicious content or opens an email attachment containing Flash media designed to exploit these vulnerabilities.

Successful exploitation of five of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The remaining vulnerability could allow an attacker to obtain confidential information.

SYSTEMS AFFECTED:

Adobe Flash Player 10.1.53.64 and earlier
Adobe AIR 2.0.2.12610 and earlier

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Six vulnerabilities have been identified in Adobe Flash Player and Adobe AIR, which include remote code execution and click-jacking. These vulnerabilities can be exploited if a user visits a website hosting malicious content or opens an email attachment containing a Flash media file designed to trigger these issues. Details of these vulnerabilities are as follows:

Five vulnerabilities caused by unspecified Memory Corruption errors could result in remote code-execution.
A click-jacking vulnerability affecting Flash Player 10 on unspecified platforms. Click-jacking is a technique that involves embedding code or a script into a web page that tricks a user into performing unintended actions. This occurs when a user mistakenly clicks on a concealed link or when the user clicks on a button that triggers the malicious action.

Successful exploitation of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate updates which have been provided by Adobe to vulnerable systems immediately after appropriate testing.
- Systems running Adobe Flash Player 10.1.53.64 and earlier versions should be updated to version 10.1.82.76.
- Systems running Adobe AIR 2.0.2.12610 and earlier versions should be updated to version 2.0.3.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Adobe:
http://www.adobe.com/support/security/bulletins/apsb10-16.html

Security Focus:
http://www.securityfocus.com/bid/42361
http://www.securityfocus.com/bid/42362
http://www.securityfocus.com/bid/42363
http://www.securityfocus.com/bid/42364

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0209
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2188
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2213
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2214
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2215
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2216